



PT LAB

Trendy v oblasti kybernetické bezpečnosti

Aneb kdo zvládl COVID lépe R/B

David Malaník, Roman Jašek

PT LAB – Penetration Testing Laboratory
Fakulta aplikované informatiky
Univerzita Tomáše Bati ve Zlíně
E-mail: ptlab@fai.utb.cz
dmalanik@utb.cz
jasek@utb.cz



R	0
B	0

Změny co přinesl COVID19/20/21/22

Fenomén perfektního mapování nových případů...

Velmi efektivní hrátky s čísly (aby to vypadalo, jak kdo chce...)

Obrovskou výzvu pro IT, jak v již mnohdy heterogenní infrastruktuře připojit navíc lidi v karanténě, homeoffice, atd..

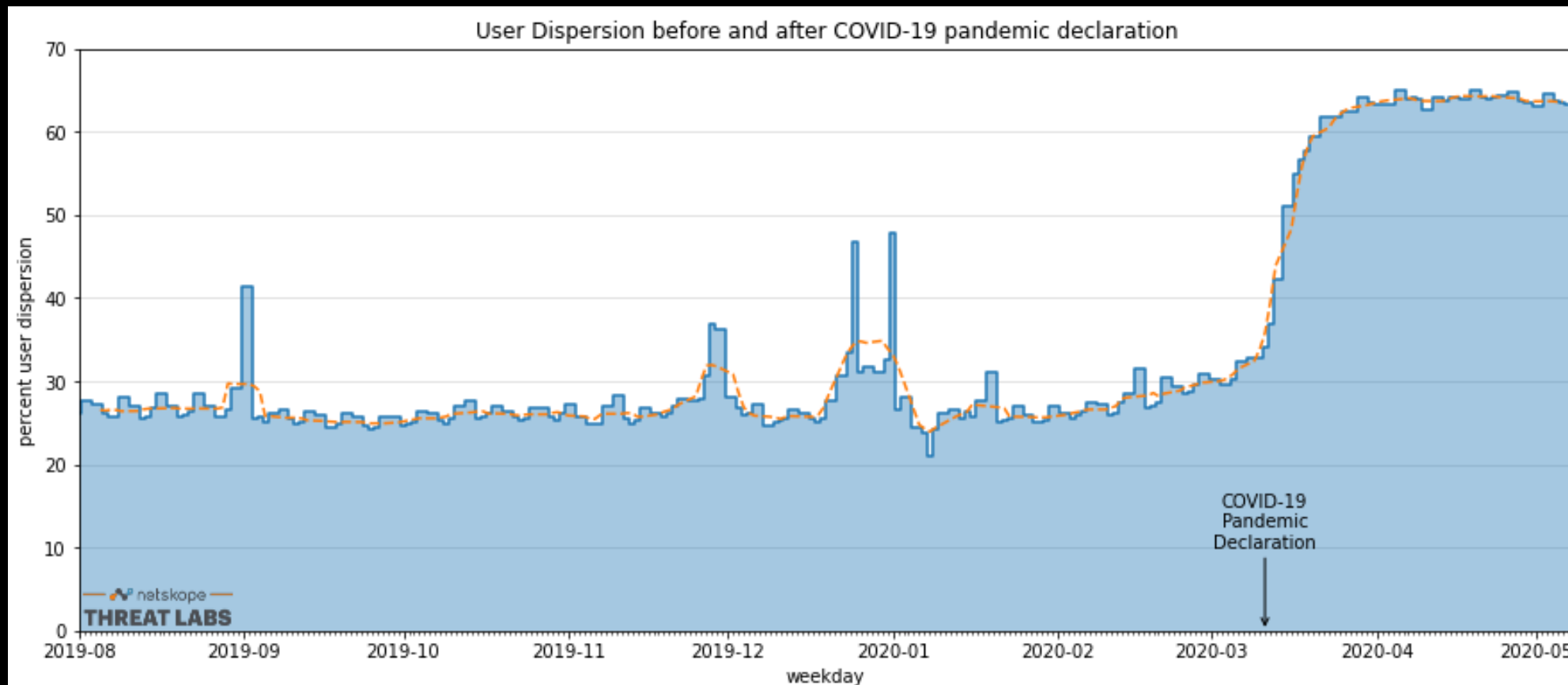
Skvělý nástroj pro útočníky – obzvláště v oblasti sociotechnických útoků



PT LAB

R	1
B	0

Homeoffice?



Enormní roztržštění infrastruktury - Potřeba vzdálených přístupů

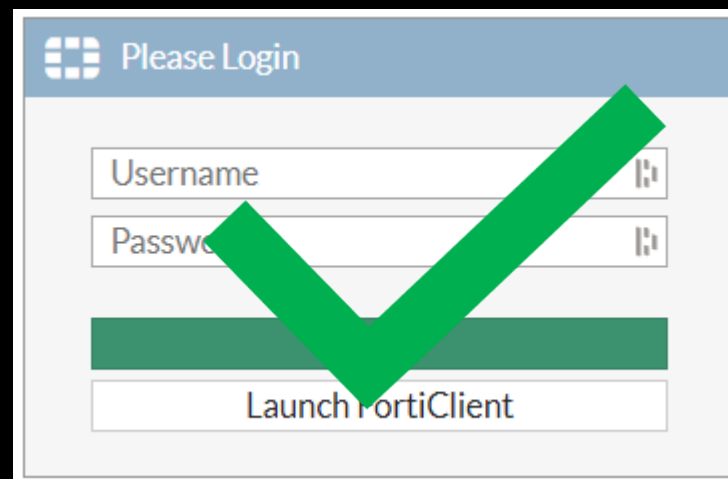
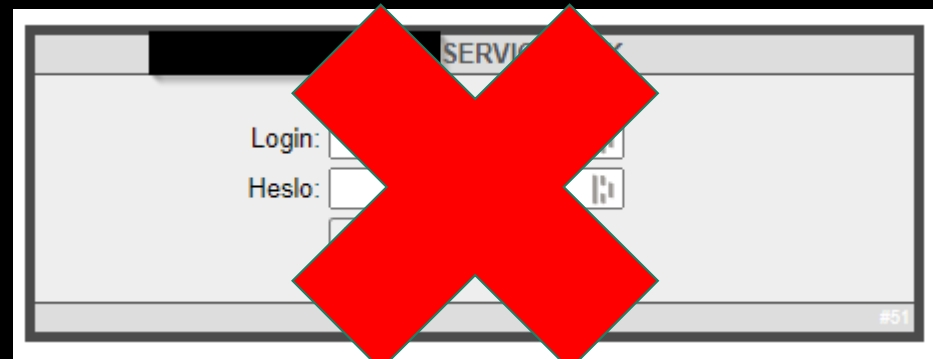
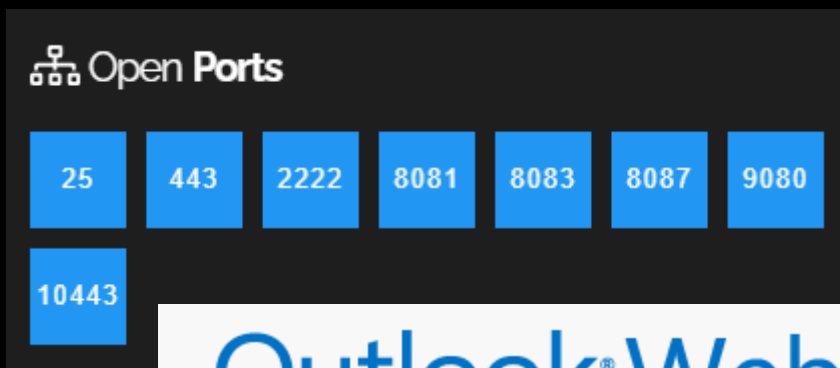


PT LAB

R	3
B	1

Nejčastější chyby

Rychlé řešení(trvalé) – port forward na WAN (> 100 CVE)



R	4
B	1

Nejčastější chyby

Mix firemních a osobních zařízení – mnohdy velmi heterogenní síť

Pracují zaměstnanci ze svých soukromých zařízení?

Máte přehled nad OS, programy, firewallem, navštívenými stránkami?
Stejný problém jako s BYOD

Mix identit – co když zaměstnanec odpoví na firemní komunikaci přes svůj soukromý účet?

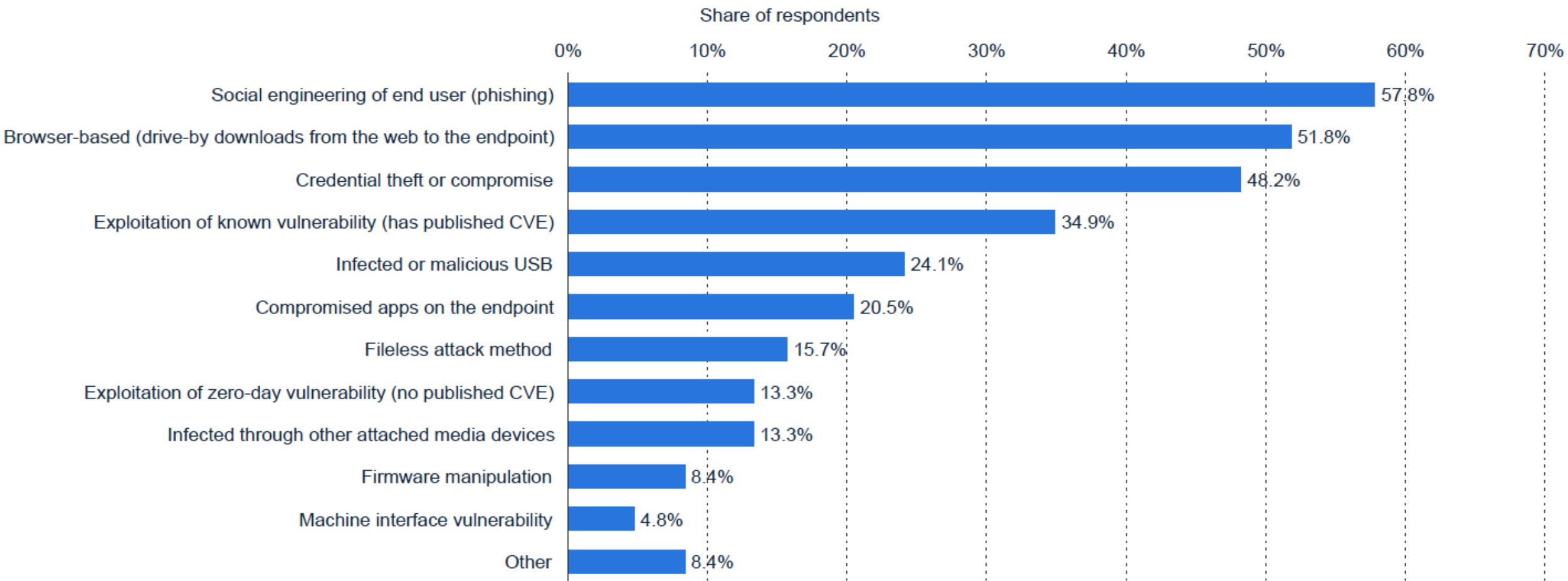
Co když „propašuje“ malware přes své soukromé aktivity?

Ransomware has seen a significant uptick so far in 2021, with global attack volume increasing by 151 percent for the first six months of



R	5
B	1

Nejčastější chyby



R	5
B	2

Příležitosti pro správce

Využití umělé inteligence (AI)

- Adaptivní reakce na incident

- Snížení počtu falešných poplachů

- Široká dostupnost HW a SW produktů pro zapojení AI

- Vývoj nextgen FW a IDS/IPS

Rozvoj AIoT/IoT

- Konečně v popředí zájmu i zabezpečení



PT LAB

PENETRATION TESTING LABORATORY

<http://ptlab.fai.utb.cz>

R	5
B	2



R	5
B	3

Příležitosti pro správce

Zero Trust

Přísnější zabezpečení dat a ochrana soukromí

Nedůvěryhodné zařízení v síti

„Nikdy nedůvěřuj, vždy prověřuj“

Umocněno v IoT

Základní koncept již z roku 2010

„paranoia“ správců již přechází i na management

R	5
B	4

Příležitosti pro správce

Využití blockchainu

Možnost decentralizované validace dat

Ověření důvěry „hlasováním“ nezávislých institucí

Zakotvení čehokoliv v čase

Možnost jednoduchého ověření existence

Energetická efektivita průmyslového blockchainu

Vytváření důvěryhodného prostředí

Výsledné skóre

R	5
B	4

Výhled a trendy do budoucna

Malware

Přechod do oblastí mobilních zařízení

Infikace IoT

Využití AI pro tvorbu a šíření

Další nárůst ransomware – vyplatí se

Větší zaměření na zdravotnictví a průmysl

Velmi lukrativní cíl -> kryptoměny

Obchod s uživatelskými daty

Výhled a trendy do budoucna

Sociotechniky

Phishingové útoky

Spearphish útoky

Zacílené na cloud

Zneužití i „non-human“ účtů

Dokonalejší podvodné kampaně

Větší zapojení sociálních sítí

Ohýbání situace a aktuálních trendů dle vlastní potřeby

Deep-fake

Čeští hokejisté nevypadli. Jenom se rozhodli bojkotovat olympijské hry

Dominik Landsman

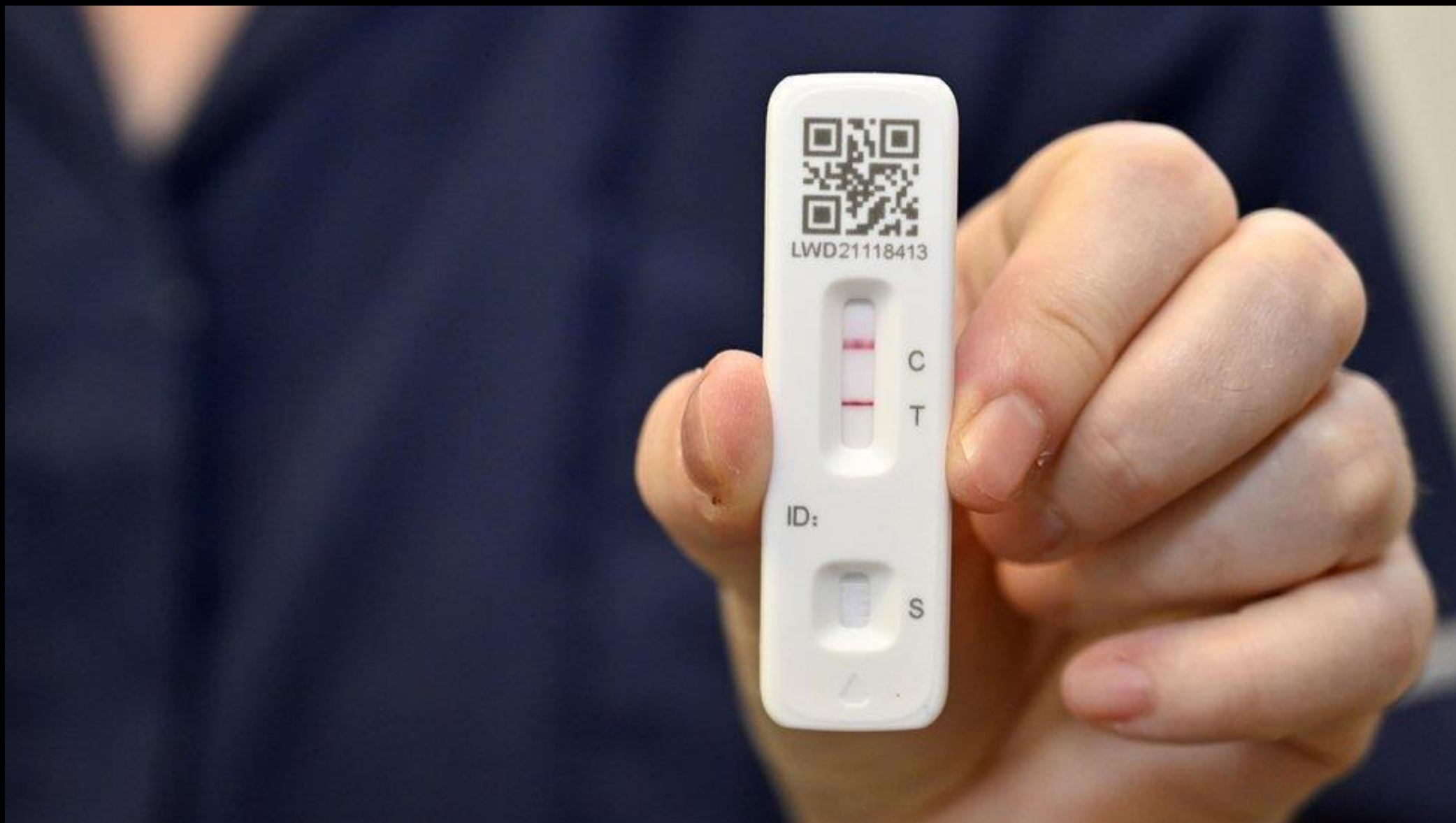
15. února 2022 • 18:30



PT LAB

PENETRATION TESTING LABORATORY

<http://ptlab.fai.utb.cz>





Příležitost k dotazům

